Propulsion Breakout Session

Time-Limited-Dispatch (TLD) for FADEC Systems

Presented to: Recurrent DER Training Attendees

By: Hals Larsen, CSTA for Prop. Control Systems

Place/Date: Arlington, TX/ May 25, 2006

Federal Aviation Administration

Time – Limited – Dispatch (TLD)

- What is it?
  - "TLD" generally refers to the capability of operating an electronic engine control system, which has redundancy, for limited periods of time with faults present in the redundant elements of the electronic control.
  - TLD Operations were established in ANE Policy Letter, ANE-1993-33.28 TLD, in Oct. 1993, Policy for Time Limited Dispatch (TLD) of Engines Fitted with Full Authority Digital Engine Controls (FADEC) Systems". Revision 1 dated June 2001.

Reference Documentation for both Turbine and Recip Engines

- What FAA documentation applies (or is helpful)?
  - The above Updated Policy Letters on TLD. The policy letter primarily apply to Turbine Engines installed on Part 25 and Part 23, Commuter Cat. Aircraft (i.e., Part 23 Class IV aircraft as defined in AC 23. 1309-1C, Fig. 2).
    - **We recommend the latest policy letter be used for engines intended for Part 27 and Part 29 Rotorcraft, as well.**
  - ANE AC 33.28-2, "Guidance Material for 14 CFR §33.28, Reciprocating Engines, Electrical and Electronic Control Systems", published Aug., 2003, contains TLD information for reciprocating engines used on Part 23 aircraft.

Other Reference Material

- SAE ARP 5107, Rev. A, Guidelines for Time-Limited-Dispatch (TLD) Analysis for Electronic Engine Control Systems, released Jan. 2005
  - It describes how to complete a system failure rate analysis using a
    1. Time-Weighted-Average (TWA) approach (using Fault Trees), or
    2. Markov Modeling Approach

    to determine the average system failure (LOTC/LOPC) rate
  - It also discusses different repair scenarios

  - 5107 is currently being updated to include a description of what elements of the engine control system should be included in the reliability (i.e., failure rate) analysis.

LOTC and LOPC Definitions

- Turbine Engines: Part 25 and 23 Commuter Cat. Aircraft and Part 27 and 29 rotorcraft
  - Loss-of-thrust-control (LOTC) is basically defined as the inability to modulate thrust between (flight) idle and 90% of maximum rated power at the flight condition.
  - Unacceptable oscillations on thrust/power.

- Reciprocating Engines: Part 23, Class I, II & III Aircraft (classes as defined in AC 23.1309-1c, Fig. 2)
  - Loss-of-power-control (LOPC) is defined as the inability to modulate power between (flight) idle and 85% of max. rated power.
  - Though not specifically cited in AC 33.28-2, consider unacceptable power oscillations to also be LOPC events.

TLD LOTC Rates

- Turbine Engines
  - For Part 25, 23 Commuter Aircraft:
    - average LOTC rate ≤ 10 events/10^6 hours
  - **LOTC rate for engines intended for Rotorcraft not specifically mentioned in TLD Rev 2 Policy Letter.**
    - Part 27 Cat. A and all Part 29 Rotorcraft: - assume average LOPC rate ≤ 10 events/10^6 hours
    - Part 27 Cat. B: a larger than 10 events/10^6 hours may be acceptable – work with ACO office for acceptable number. 10/10^6 hours is always good default number…

LOTC Rates

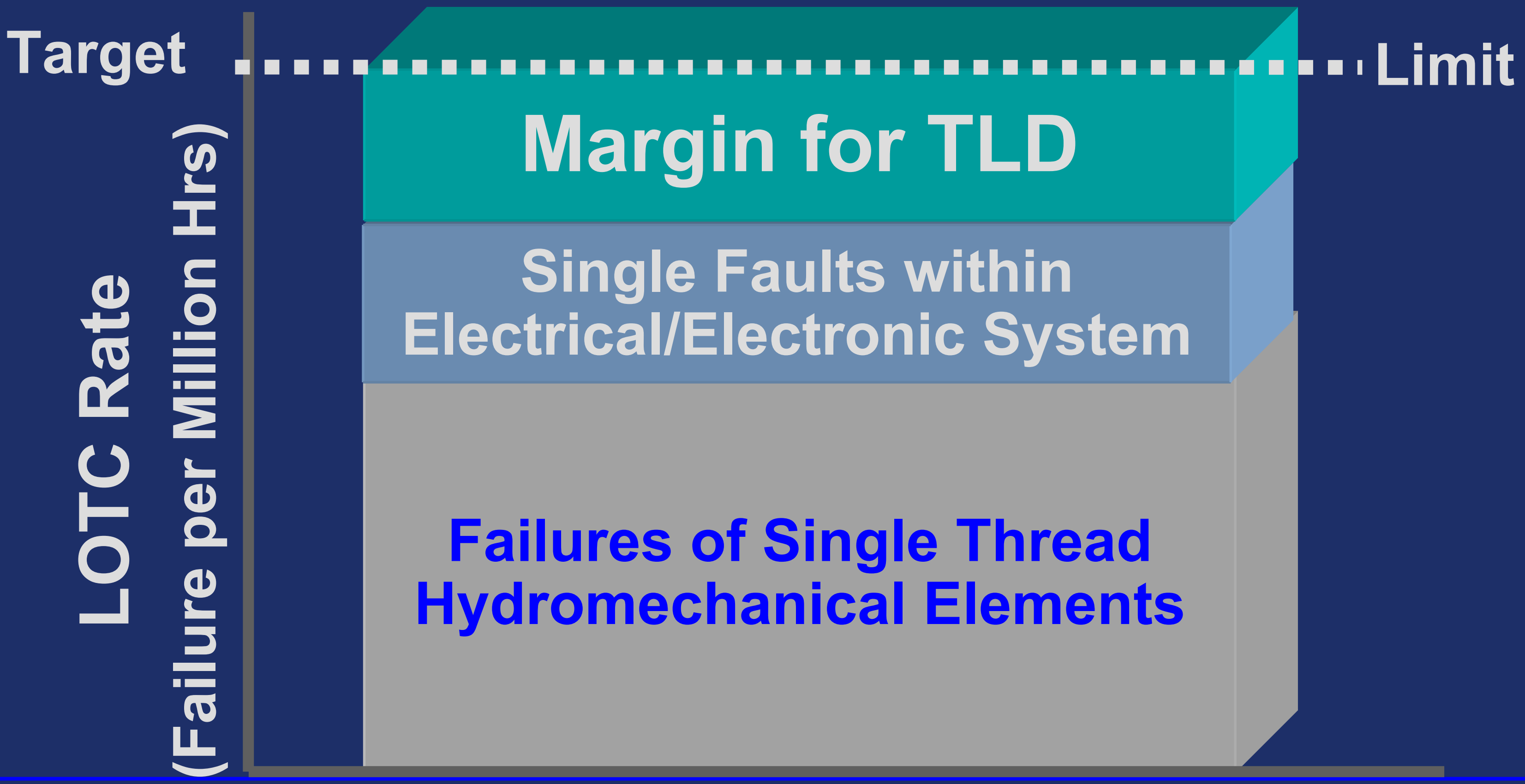
- Turbine Engines
  - TLD Rev 2 policy letter indicates that for Part 23 Class I, II, III aircraft, average LOTC rate may be reduced, ≤ 25 events/10^6 hours MAY be acceptable.
    - However, EASA is appearing to require an average LOTC rate ≤ 10 events/10^6 hours for all turbine engines – regardless of the application
    - A common FAA/EASA LOTC target for these part 23 aircraft is currently under discussion
  - Applicants encouraged to design to the ≤ 10 events/10^6 hours for turbine engines.

TLD Definitions

- Reciprocating Engines
  - AC 33.28-2 organizes the LOPC rate by sub-system function:
    - Less than 15 failure events per 10^6 operating hours for each of the three sub-system functions of fuel flow, ignition and turbocharger.
    - If there are more than 3 sub-systems functions, the upper limit is still 45 per 10^6 hours of operation.

Time Limited Dispatch (TLD)

TLD Visualized



Target
Limit
LOTC Rate
(Failure per Million Hrs)
Margin for TLD
Single Faults within Electrical/Electronic System
Failures of Single Thread Hydromechanical Elements

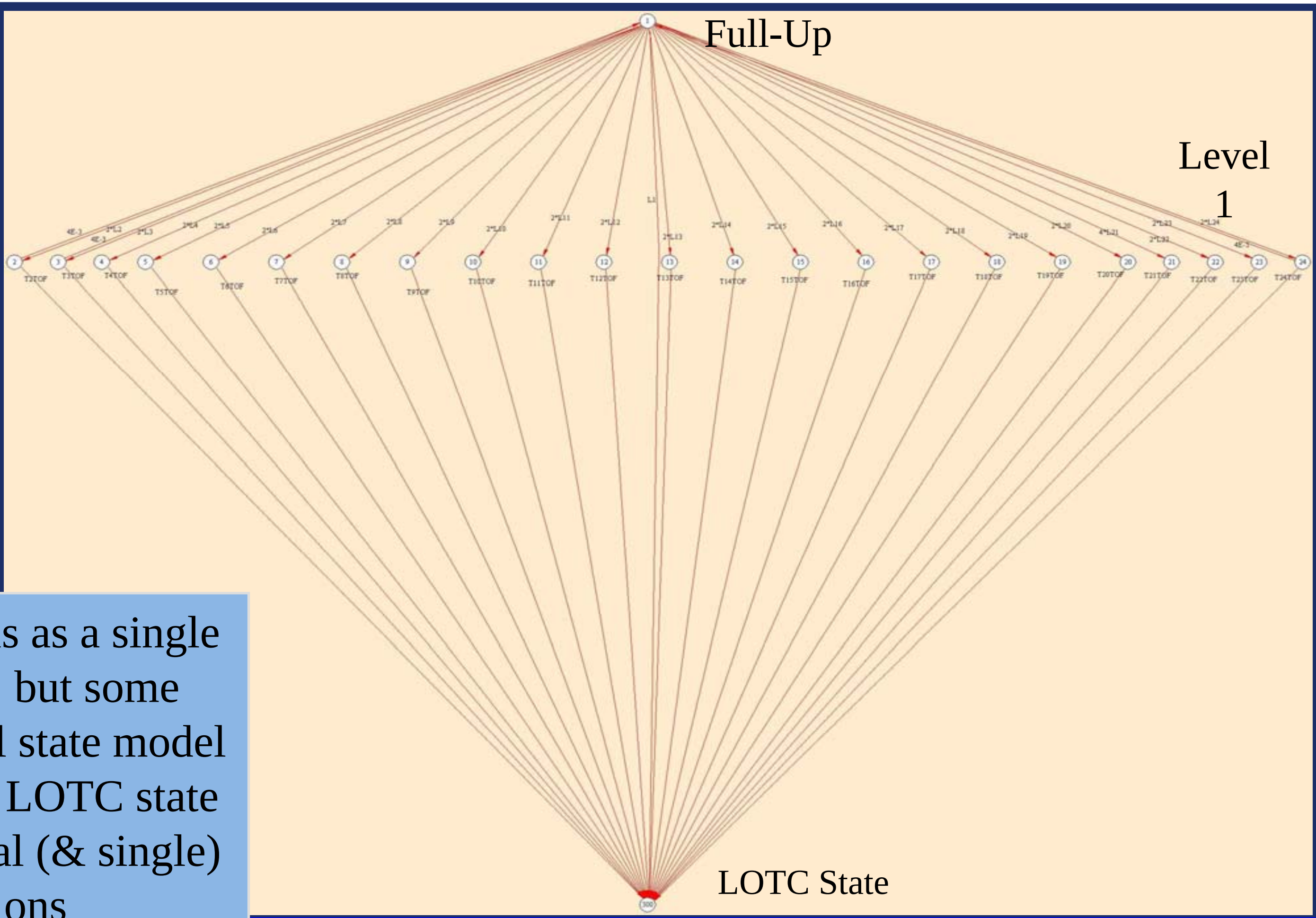
What are the best practices regarding the application of TLD for the engine control systems?

- Develop a Fault Tree Model (use the time-weighted-average approach to determine the average LOTC/LOPC rate) or a Markov Model (MM) to estimate the average failure rate of the control system.
  - See Jan. ’05 SAE ARP 5107 Rev. A for a discussion and examples of both approaches.

What about Model Complexity?

- For both the Time-Weighted-Average Fault Tree approach and the Markov Modeling approach:
  - For repair times that are much more frequent than the MTBF times of the various dispatchable system fault states, a single fault model is an adequate representation of the system - single fault models are ones where each single fault state is simulated AND the next faults considered are "only those that result in an LOTC/LOPC event".

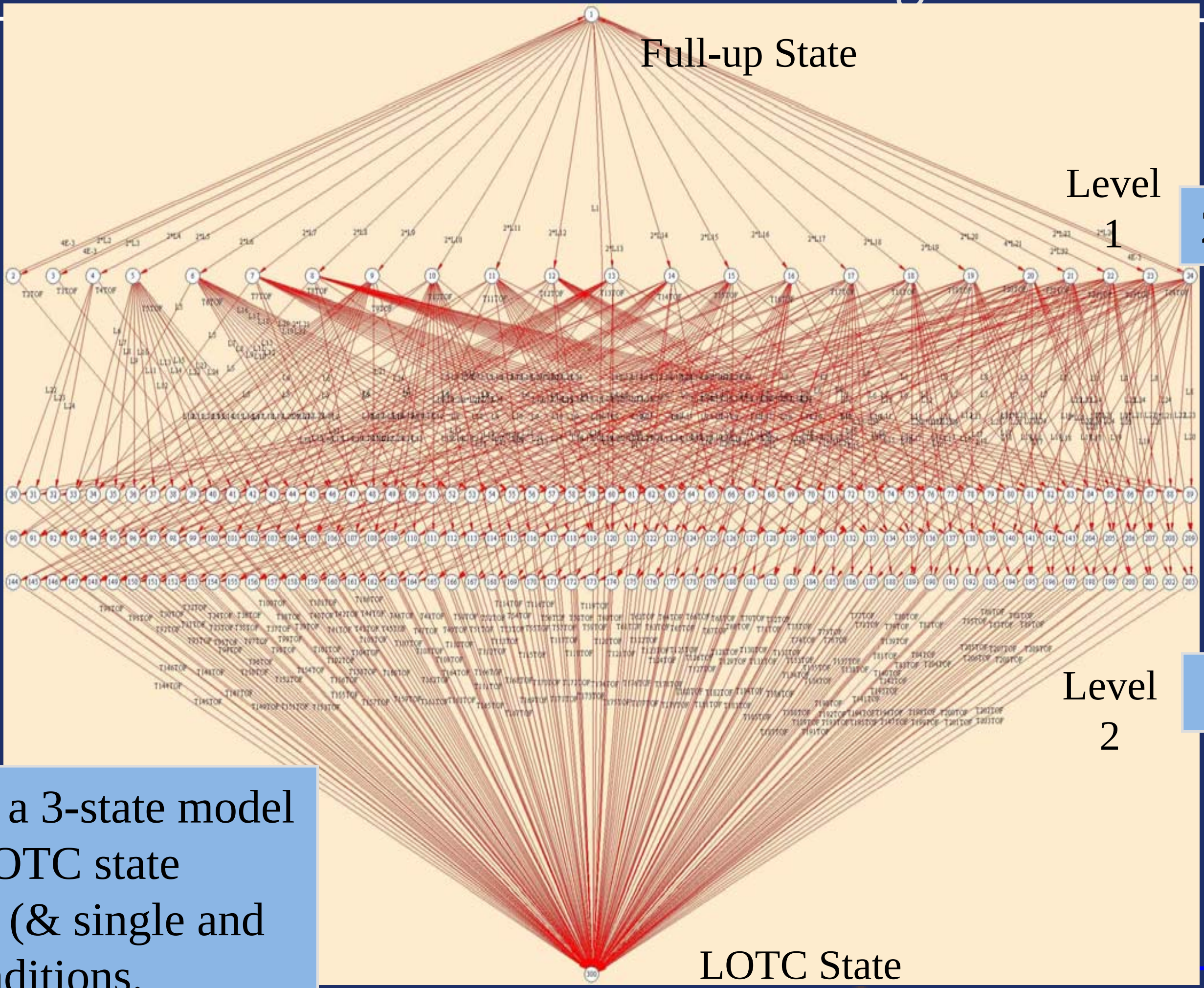
Generic Single State Model



I refer to this as a single state model, but some call it a dual state model because the LOTC state contains dual (& single) fault conditions

Generic Dual State Model

Cross-channel resource-sharing



Full-up State

Level 1

23 States

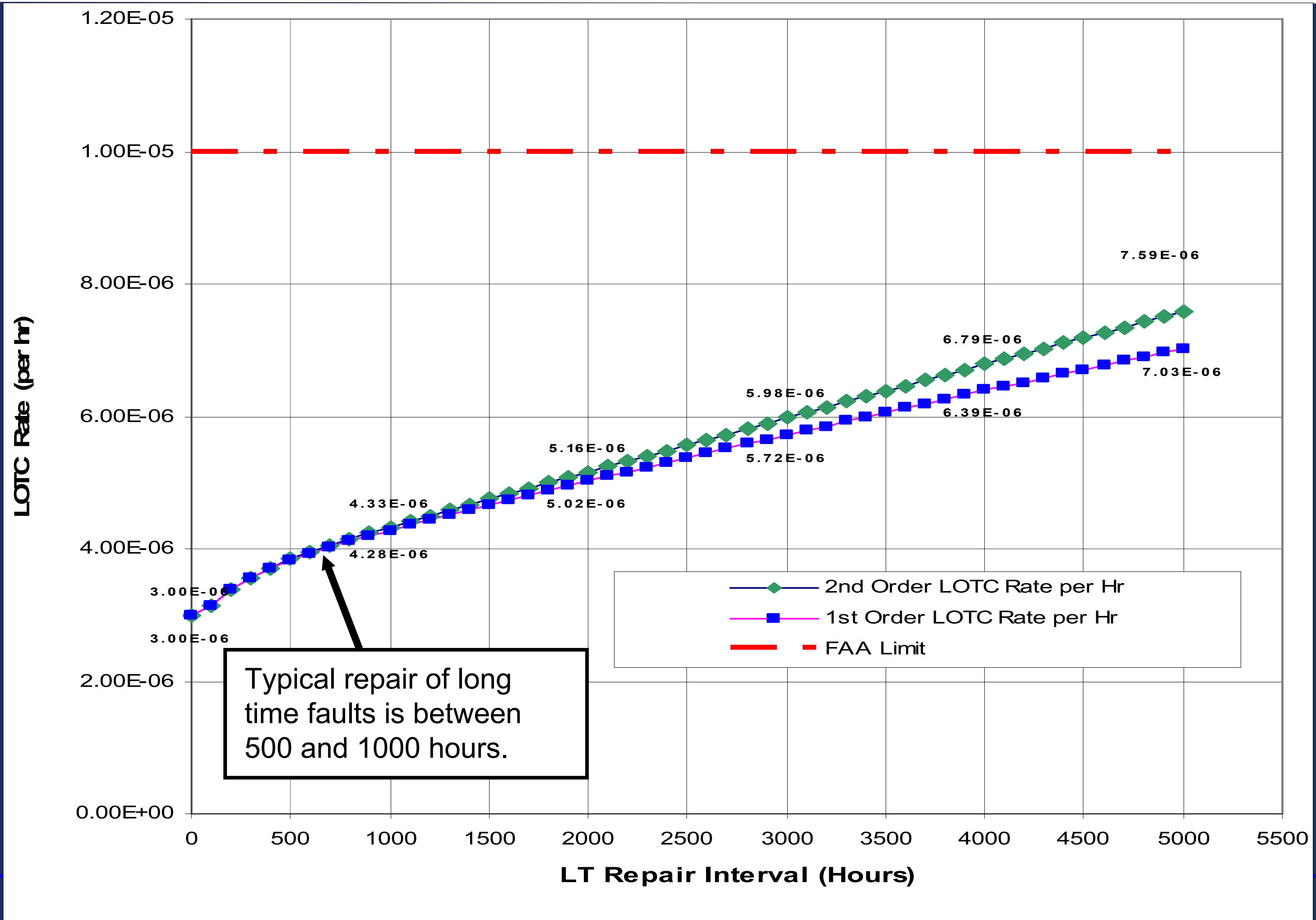
Level 2

180 States

LOTC State

Some call this a 3-state model because the LOTC state contains triple (& single and dual) fault conditions.

Comparison of Single & Dual State Model Results



Typical repair of long time faults is between 500 and 1000 hours.

Federal Aviation Administration

What are the best practices regarding the documentation of TLD for engine control systems?

- Document the system analysis for FAA review and approval of TLD operations.
  - The display and repair requirements, including the TLD time limits for dispatchable faults, should be contained in the Airworthiness Limitations Section of the engine's Instructions for Continued Airworthiness.

    (This should ensure that the operator's are aware of engine's control system installation requirements and limitations.)

    - Example of display requirements: A "No Dispatch" condition must be displayed to the flight crew

Do all programs use a TLD summary document to explain the dispatch criteria?

- **No.** Previous programs have not done this AND this has caused some difficulty
  - Some applicants put the full LOTC reliability analysis, and the resulting TLD dispatch times, into one document – which the applicant considers proprietary to the company. Thus, the source of the dispatch criteria is not available to the operators.

- **Recommendation:** The applicant should create a summary document that contains a table of the various system faults and the required repair times (i.e., TLD dispatch times for those faults.

Should the TLD analysis report only address control systems failures that lead to LOTC events, or should it include all the secondary system faults, such as loss of display information ?

- For Part 25, Part 23-Class IV, and Part 27 and 29 applications, the analysis should include all control system faults that lead to LOTC events as well as secondary system faults, such as the loss of, or misleading transmission of display parameters that are processed by the electronic control unit - if the loss of or misleading display of that parameter would result in a crew initialed IFSD.
- It is recognized that in Part 23 I, II and III aircraft, the loss of display information will probably not lead to an engine IFSD. However, false indications may lead to a pilot initiated IFSD.

Do all TCDS documents contain a note that explicitly indicates TLD approval?

- No. When the TCDS does not indicate that TLD operations have been approved, then full-up control system operation is required at each dispatch.

- NOTE: When the TCDS indicates that TLD operations have been approved, the TLD time limits do not have to be stated on the TCDS. The engine Limitations Sections of the ICA's is the place to put them. (See ANE Rev 2 Policy letter on TLD.)

Do applicants show the TLD summary tables in the control systems' Plan for Software Aspects of Certification (PSAC)?

- No. The TLD analysis and time limits established for TLD operations should be contained in other, separate documentation

What do aircraft maintenance documents have to say about TLD and how is it applied?

- For transport aircraft, the aircraft’s maintenance documents will contain the engine’s Limitations in a section titled “Maintenance Sensitive Items”, or similar title. However, this is not required. Engine Limitations stand on their own.
  - Part 121 operators have to show that their operation and maintenance plans for the aircraft comply with all aircraft and engine Limitations.
  - It is expected that Part 91 and 135 operators of GA aircraft comply with these limitations as well.

What do aircraft maintenance documents have to say about TLD and how is it applied?

- Can the aircraft manufacturer be more restrictive with regard to TLD time limits?
  - Yes. If the aircraft manufacturer wants to be more restrictive with TLD operations than the limitations approved for the engine, that is always permissible.
  - In this case, the aircraft manufacturer should place the more restrictive requirements in the aircraft's Limitations section of the aircraft's Instructions for Continued Airworthiness.

FADEC System Maintenance Scenarios

- For all Turbine engine applications, repair of FADEC system faults can generally be grouped into 2 fault group/dispatch categories:
  - Short Time (ST) Faults
    - As the name implies, these are faults that have to be repaired within a short time interval, like 10 days or 125 flight hours.
  - Long Time (LT) faults
    - These are faults that require repair within a longer time interval, such as 500 flight hours.

  - See SAE ARP 5107 for a more detailed discussion of these fault/dispatch categories

FADEC System Maintenance Scenarios

- For GA airplanes with recip engines, FADEC systems use just one time interval for dispatch.
  - 20 flight hours as (recommended) given in AC 33.28-2

TLD Time intervals:
What has to be fixed? and when?

- Turbine & Recip Applications:
  - Electronic control applications must have a cockpit display which indicates a "no dispatch" fault condition.
- Turbines:
  -Most turbine engine applications show have a flight deck/cockpit indication of a ST dispatch condition. LT faults are generally handled with a periodic inspection/repair approach.
- Recips:
  - If a cockpit display of a dispatchable fault condition is not available, an inspection for FADEC system faults after each flight is recommended.

Repair Intervals (or times) used in the TLD analysis

- Turbine Applications:
  When using the (planned maintenance), periodic inspection/repair approach (generally for LT faults):
  - If the time of occurrence of the faults not known, the system should be cleared of all faults in the group being addressed (i.e., generally LT faults) by using an inspection/ repair interval that is not greater than twice the time-since-fault “time limitation” specified for faults in that group.
  - This will ensure that the “average” operating time of the faults being addressed using the inspection/repair strategy does not exceed the maximum specified time-since-fault operating time for those faults.
  - See ANE TLD policy letter for detailed discussion

When using the planned maintenance, periodic Inspection/Repair Approach

- If the faults in the periodic inspection/repair group (generally LT faults) have an "approved" time/date stamp associated with the fault AND the operator wants to handle all faults in the group individually, then
  - each fault should be repaired within the operating time limitation given for that group of faults, and
  - the operating time "starts" with the time/date stamp for the fault.

  - When using this approach, the periodic inspection time for faults should be no greater than the time limitation for faults in that group.

Summary

- For more detail on TLD and TLD analyses, please refer to:
  - For Turbine Engines: TLD Policy Letter, ANE-1993-33.28TLD-R1, dated June 29, 2001 & AC 33.28-1
  - For Recip Engine: AC 33.28-2
  - For TLD Analysis Approaches and other information:

    SAE ARP 5107 Rev A , Guidelines for TLD Analyses for FADEC Systems

If you have questions, contact your ACO person

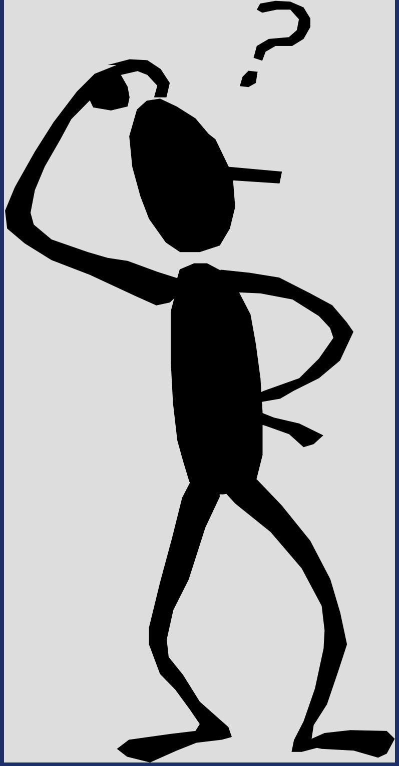
If further investigation is needed,
the following individuals may be contacted for assistance:

Gary Horan @ 781-238-7164
e-mail: gary.horan@faa.gov
or
Norm Brown @ 781-238-7181
e-mail: normal.brown@faa.gov
or
Mark Rumizen @ 781-238-7171
E-mail: mark rumizen@faa.gov

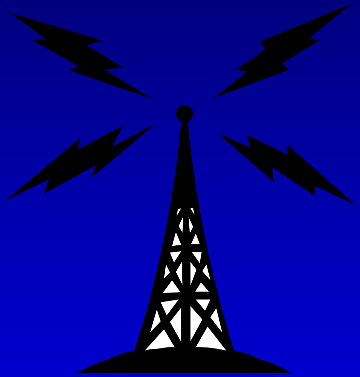
or

Hals Larsen @ 425-917-6582
e-mail: hals.larsen@faa.gov

Questions



Maintenance Associated with FADEC System Lightning Protective Elements



Presented to: Recurrent DER Training Attendees

By: Hals Larsen, CSTA for Prop. Control Systems

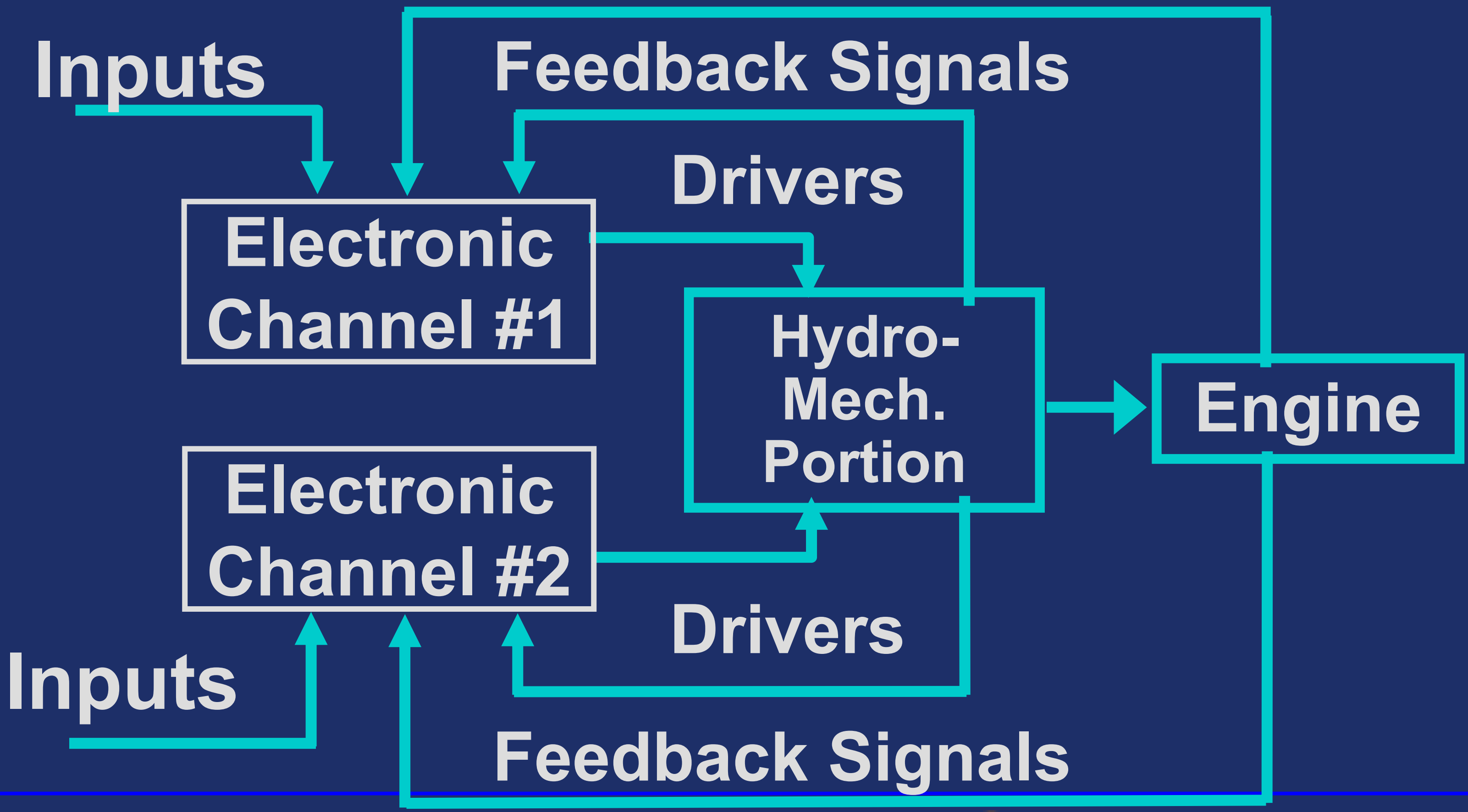
Place/Date: Arlington, TX/ May 25, 2006

Federal Aviation Administration

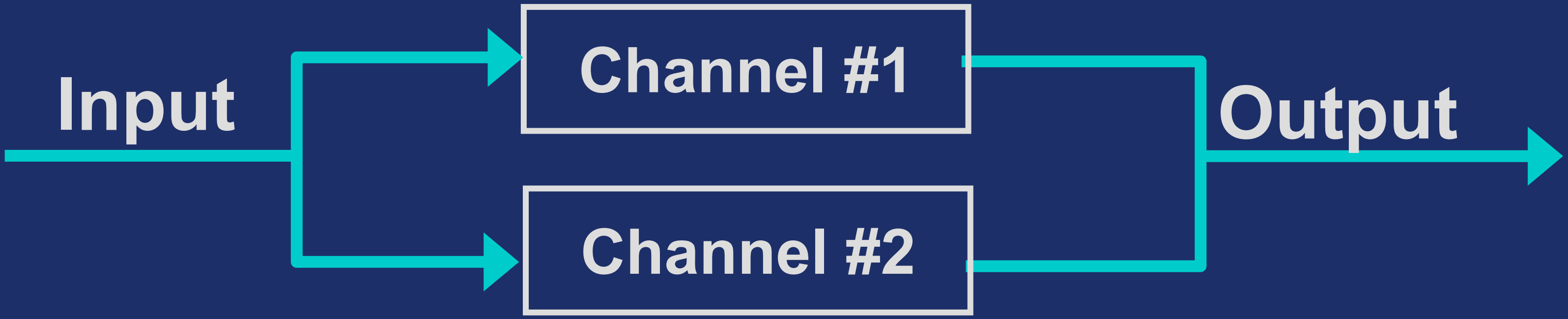
Potential Latent Failure in the Lightning Protective Components

- There has been discussion lately of whether the use of a unit’s MTBF (for detected failures) is adequate for addressing repairs to undetected failures in the unit’s lightning protective components.
  - The concern is that multi-units in a redundant system could have undetected failures in their protective components, and if those units are not repaired, a lightning strike could cause “all” units to fail – with potentially Hazardous or Catastrophic results.

Typical FADEC System



Considering just the electronic units…



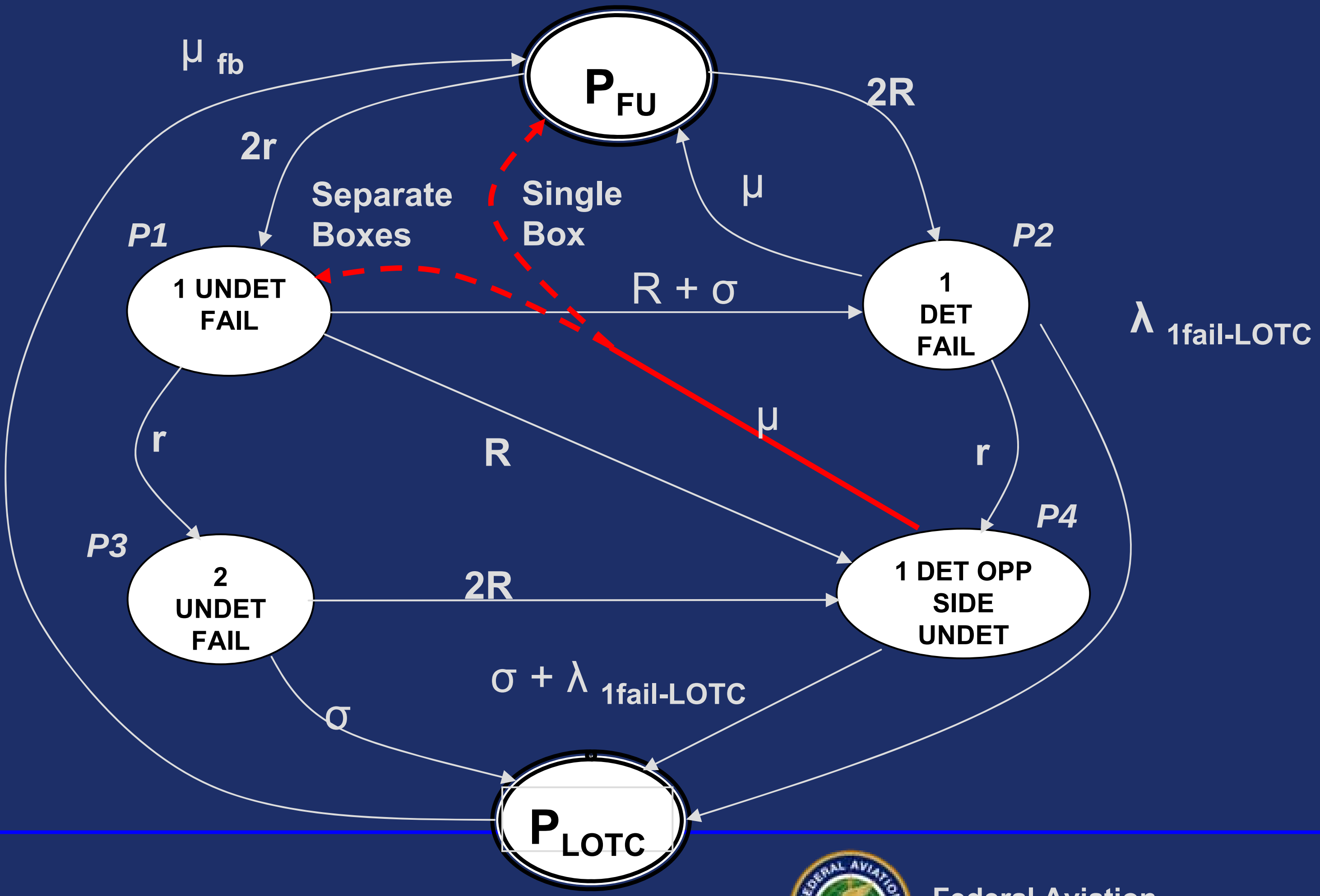
- Assume that each channel has a failure rate of $50*10^{-6}$ events/hr. (an MTBF for repair of 20,000 hours. This is quite reasonable.)
- Assume that 10% of a channel's components are for lightning protection (a very conservative (high) estimate).
- Assume that 10% of those failures are undetectable (also a high estimate)
- Then (again being very conservative) 1% of the protective components have failures which are undetectable

There are 2 system configurations…

- Both channels are in one box.
  - In this case, both channels have failures in their undetected components (associated with lightning protection) repaired when either channel has a detected fault and the box is “opened” for repair.

- The channels each have their own, separate boxes
  - In this situation, undetected failures in the lightning components of the channel NOT being repaired for a detected failure would remain in the system. That is, undetected failures in the protective components will only be repaired (in a channel) when that channel undergoes repair for a detected failure.

Markov Model for both configurations



Federal Aviation Administration

The System Equations are:

Conservation Eq. $P_{FU} + P_1 + P_2 + P_3 + P_4 + P_{LOTC} = 1$

P1 State Eq. $2r*P_{FU} + \mu*P4 = (\sigma + 2R + r)*P_1$ (If both channels are in the same unit, there is no $\mu*P_4$ term in this equation.)

P2 State Eq. $2R*P_{FU} + (\sigma + R)*P_1 = (\mu + \lambda_{1FAIL-LOTC} + r)*P_2$

P3 State Eq. $r*P_1 = (\sigma + 2R)*P_3$

P4 State Eq. $R*P_2 + 2R*P_3 = (\sigma + \mu + \lambda_{1FAIL-LOTC})*P_4$

The failure rate of the system is:

$$\lambda_{LOTC} = \frac{\lambda_{1fail-LOTC}*(P_2 + P_4)/P_{FU} + \sigma*(P_3 + P_4)/P_{FU}}{1 + (P_1 + P_2 + P_3 + P_4)/P_{FU}}$$

Assume the following failure rates…

- $R = 5*10^{-5}$ events/hr (Chan. fail rate for detected failures)
- $r = 5*10^{-7}$ events/hr (Chan. fail rate for undetectable failures)
- σ = lightning strike rate
- μ = average repair rate for a failed channel (i.e., $1/T_{REPAIR}$)
  - This assumes TLD is being used for the system
- $\lambda_{1fail\text{-}LOTC} = 3.4*10^{-6}$ (failure rate from one channel having a detected failure to the sys fail (LOTC) state)

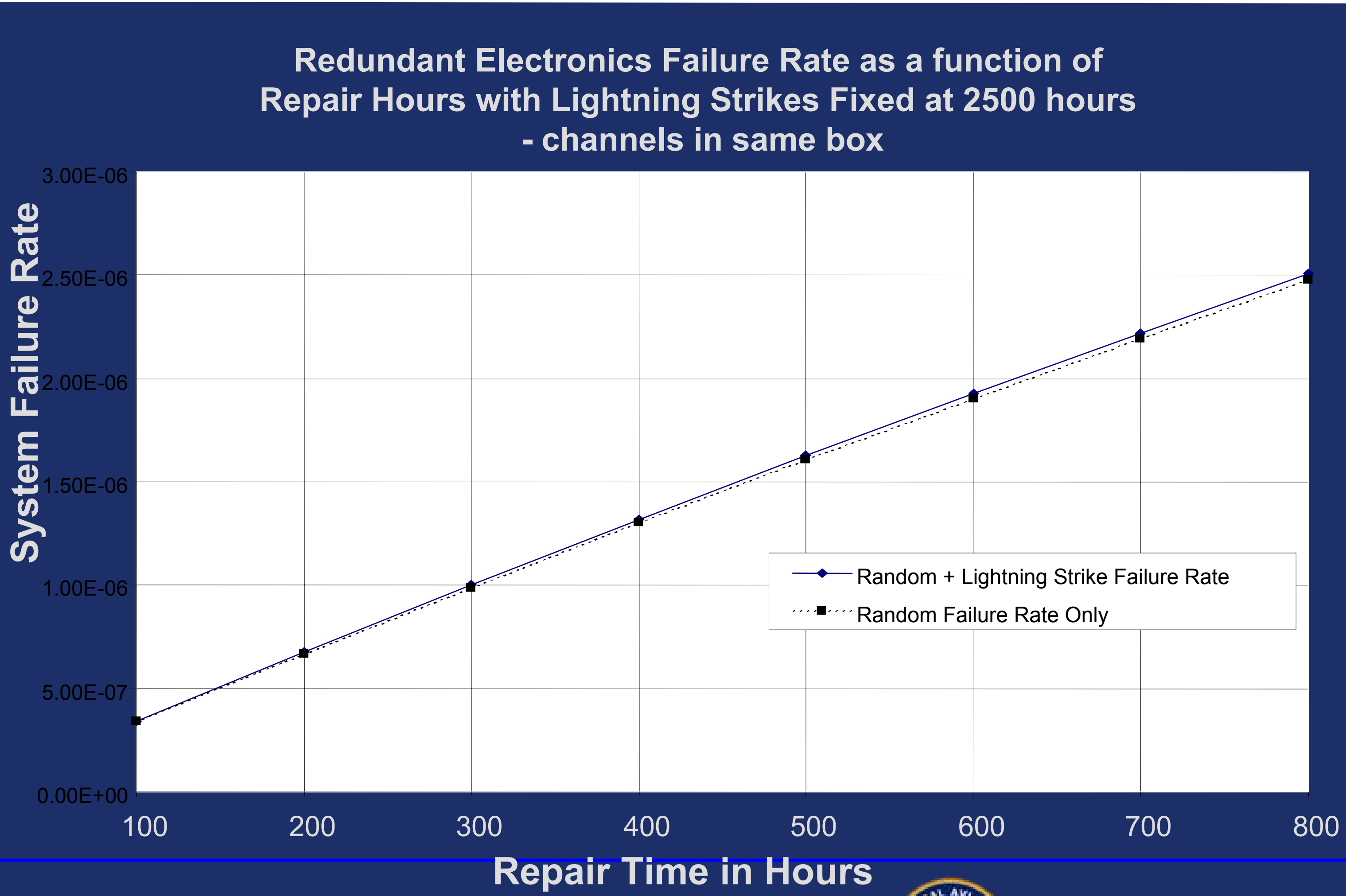
Assumptions

- The analysis assumes that the two channels – even when in the same box – are electrically isolated.
- That a channel (in control) with undetected failures in the lightning protective components – when “hit” with a lightning strike of sufficient magnitude, will fail AND the control will revert to the other channel – when the other channel is operative.
- That lighting strikes of a severe magnitude occur every 2500 hours. This is very conservative. Transport reported events indicate a 6,00 to 10,000 hour mean-time-between-strikes. Severe strikes are only estimated to occur every 20,000 hours, or more.

Failure Rate Addition due to lightning strike events

- The calculations show that the increase in the system failure rate due to lightning events comes primarily from the condition where one channel is failed and the other channel has failures in the lightning protective components – and then a lightning strike (of sufficient magnitude) occurs.
  - The results show that the failure rate due to lightning strike events is highest when the lightning strike rate is frequent.
  - The condition of having both channels with undetected failures in their lightning protective components – and then suffering a lightning strike event - adds little to the system lightning strike failure rate.

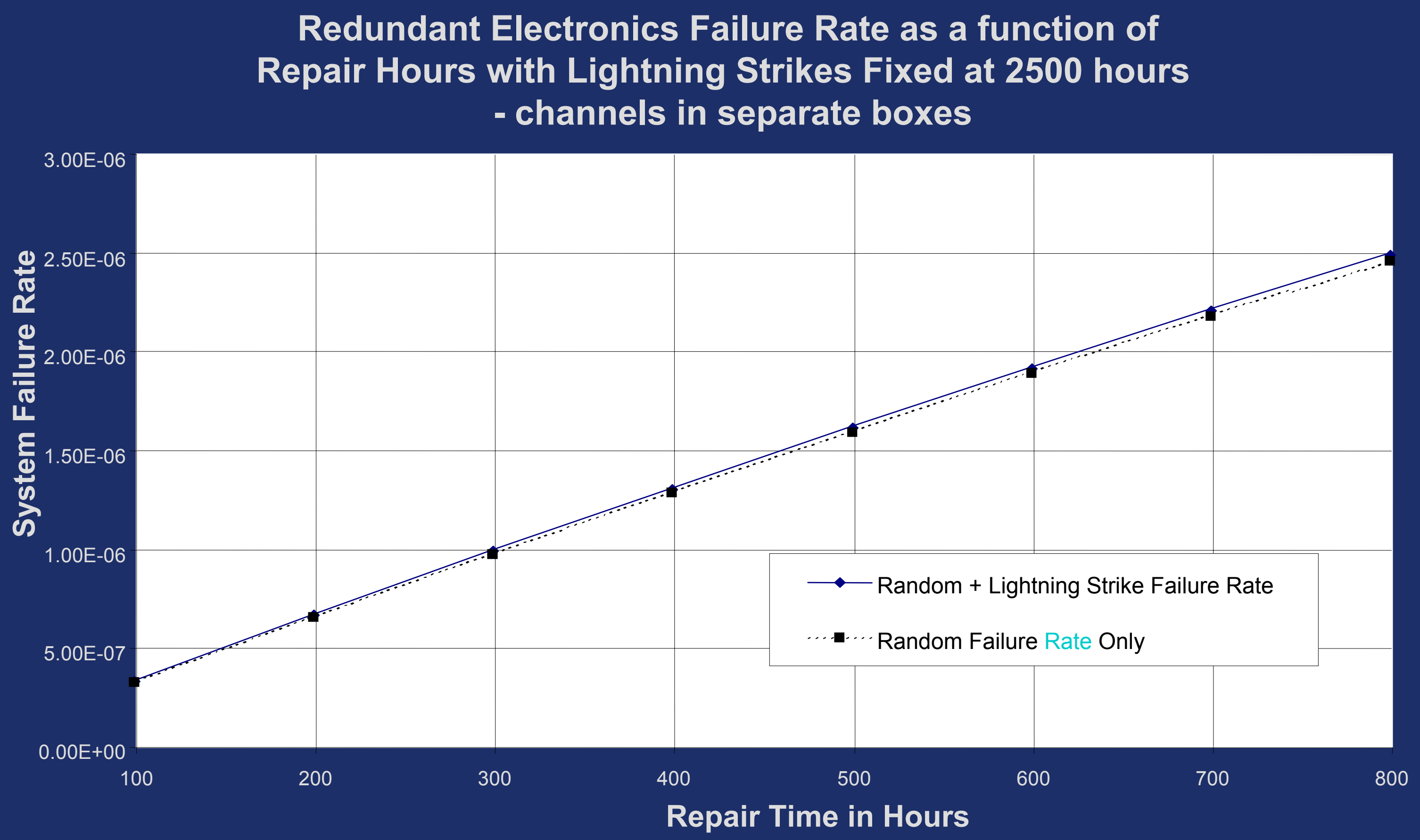
Failure Rate vs. Repair Time



Units in Separate Boxes

- The answer is essentially unchanged. The increase in the failure rate due to the channels being in separate boxes is quite small.

Failure Rate vs. Repair Time



Conclusions

- The concern for FADEC system failures due to undetected failures in the lightning protective components – and encountering a lightning strike - offers no significant impact to the system’s LOTC rate.

- The “repair rate” has a much greater impact on the system failure rate. But… Applicants should give this consideration,
(i.e., there should be some “indication” in the certification documentation that this subject has been given consideration).

Recommendations/Requirements

- The EEC should be designed so that the lightning protective devices can be inspected/tested for operability when the box/unit is opened for repair of a detected fault.

- There should be a “requirement” in the Electronic Control Unit’s Component Maintenance Manual (CMM) to test/check the integrity of the lightning protective devices when shop repair of unit is performed.

Questions